Kentucky Governor's Office for Technology

Security Awareness Newsletter

Published by the GOT Division of Security Services

November 2003 **Volume 1, Issue 6**

Inside this issue:

The Importance of Monitoring System Logs

A crucial part of ensuring network security is to routinely monitor the system event logs. By examining the logs on a regular basis, you can identify problems before they cause loss of service.

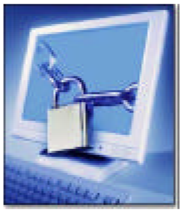
Security logging is usually enabled by default; however, administrators should verify that all logging has been turned on. Windows-based servers have several logs that should be monitored:

— **Application Logs**—contains events logged by application or programs, e.g. McAfee Anti-Virus.
— **Security Logs**—records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects.
— **System Logs**—contains events logged by system components, i.e., the failure of a driver or other system component to load during startup.
— **Domain Controller Logs (2)** for computers configured as Domain Controllers:
Directory Service Log—contains events logged by the Windows directory service, i.e., connection problems between the server and the global catalog.
File Replication Service Log—contains file replication failures and events that occur while domain controllers are being updated with information about sysvol changes
— **DNS Logs** for computers configured as DNS servers. Contains events associated with resolving DNS names to Internet Protocol (IP) addresses.
— **IIS Logs** for computers configured as web servers.

Certain log events throw up red flags and should be investigated immediately. These include failed logons, invalid user names or passwords, account lockouts, logons at unusual times such as the middle of the night, and failed resource access events.

If you happen to be running a Windows-based network, Microsoft offers various tools to monitor server performance. Some of the tools are built into Windows 2000 or IIS 5.0 and others are included in the Windows Resource Kit CD. For more information on monitoring logging, check out this Microsoft site.

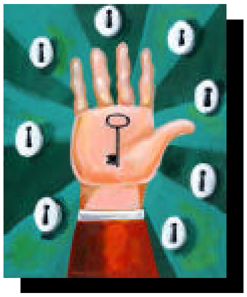
GOT Computer Security Day—December 1, 2003



All GOT staff and contractors are invited to attend this year's celebration of Computer Security Day, Monday, December 1, from 11:30 to 1:00 in Cold Harbor Training Rooms A & B. This year's event will include games with a computer security theme and free hot dogs, chips, and drinks. Prizes will also be awarded to lucky winners. Contact Julie Schuller at 564.8716 to register.

Did you know . . . According to the 2003 Deloitte & Touche Global Survey, 39% of respondents acknowledged that their systems had been compromised in some way during the last year.
— 16% report attacks from an external source.
— 10% report attacks from an internal source.
— 13% report attacks from both sources.

Visitor Access to GOT Buildings

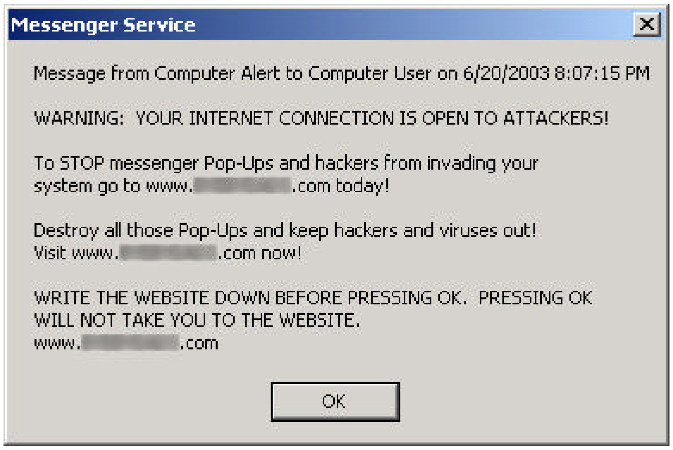


In order to keep GOT facilities adequately secured, policies have been developed that address physical access to these buildings, particularly visitor access. While having appropriate access policies in place is important, it is also crucial that all GOT staff be aware of their surroundings, especially unfamiliar faces in their work areas or people who appear to be wandering around unescorted. If you do encounter someone whom you suspect to be an unauthorized visitor, notify the security guard immediately (or supervisor if the guard is unavailable) and report the incident to Security Services via a GOT Security Incident Reporting Form (GOT-F012).

Listed below are procedures that all GOT facilities are required to follow when granting visitor access:

— All visitors must provide a state ID or other picture ID for positive identification.
— All visitors are required to sign in and out when accessing GOT buildings. The visitor must record the agency/company they represent, as well as the GOT employee/contractor they are visiting.
— Visitors to the CDC must obtain a visitor badge and display it at all times.
— Visitors must be under escort when accessing secure areas of the building.
— All children must be accompanied by an adult who has completed the sign in procedure.
— Vendors and agency personnel that have been issued a GOT security badge do not need an escort when in GOT facilities; however, they must still adhere to the sign in/out procedures required of all GOT staff.

Relief from Pop-ups



Message from Computer Alert to Computer User on 6/20/2003 8:07:15 PM

WARNING: YOUR INTERNET CONNECTION IS OPEN TO ATTACKERS!

To STOP messenger Pop-Ups and hackers from invading your system go to www.[redacted].com today!

Destroy all those Pop-Ups and keep hackers and viruses out! Visit www.[redacted].com now!

WRITE THE WEBSITE DOWN BEFORE PRESSING OK. PRESSING OK WILL NOT TAKE YOU TO THE WEBSITE.
www.[redacted].com

We are all familiar with those annoying advertising pop-ups that we run across while surfing the net; however, there is a new breed of pop-up out there that is taking advantage of the Windows messenger service built into the Microsoft Windows 2000 and XP operating systems. *(Windows messenger service should not be confused with instant messaging.)*

This MS feature was originally designed for network administrators to communicate with users via pop-up text messages; however, hackers soon discovered the feature and found a way to use it to broadcast messages across the Internet. Advertisers are now taking advantage of this to pitch their wares, making many users frustrated over the daily deluge of unwanted pop-up messages. Microsoft has no plans to do away with the Windows messenger service and states that it does not pose a security risk, declaring that it does not allow advertisers to execute code or do anything malicious.

To disable the Windows messenger service and stop related pop-ups, follow the instructions below:

— From the START button, go to CONTROL PANEL.
— Click on ADMINISTRATIVE TOOLS and double click SERVICES.
— Scroll down to MESSENGER. Double click MESSENGER.
— Reset Startup Type to DISABLED.

Please note that these instructions may vary depending upon the version of Windows you have and only pertain to Windows 2000 and XP. Disabling Windows messenger service will not prevent other browser-related pop-ups. If you have questions or need assistance, please consult your network administrator or other technical resources staff.

SANS/FBI's Top 20 List

The SANS Institute and the FBI National Infrastructure Protection Center (NIPC) recently updated their list of the Top 20 Internet security threats. The list details vulnerabilities for both Windows and Unix platforms, which are the most predominate operating systems in use today. Hackers can use these weaknesses to run scripts to gain back door access to a network or to run denial of service (DoS) attacks. Experts recommend that network administrators concentrate on applying the appropriate fixes for these weaknesses before any other network fixes. For more information, check out the SANS website.

Top Windows Vulnerabilities

Internet Information Services (ISS)
Microsoft SQL Server (MSSQL)
Windows Authentication
Internet Explorer (IE)
Windows Remote Access Services
Microsoft Data Access Components (MDAC)
Windows Scripting Host (WSH)
Microsoft Outlook Express
Windows Peer to Peer File Sharing (P2P)
Simple Network Management Protocol (SNMP)

Top Unix Vulnerabilities

BIND Domain Name System
Remote Procedure Calls (RPC)
Apache Web Server
General Unix Authentication Accounts with No
 Passwords or Weak Passwords
Clear Text Services
Sendmail
Simple Network Management Protocol (SNMP)
Secure Shell (SSH)
Misconfiguration of Enterprise Services NIS/NFS
Open Secure Sockets Layer (SSL)

Spam Remedy

Foreword: The information provided in this article is intended to be a possible solution to reduce the effects of unwanted, unsolicited email (aka Spam) and is intended for network administrators. The instructions below require the editing of the system registry, which should only be undertaken by a network administrator or other technical support staff. Users should never attempt this type of modification themselves.

There is a solution for those who are tired of being bothered by Spam emails that contain porn pictures. Outlook 2003 has a built-in feature that allows users to disable graphics to stop those vulgar porn pictures from displaying. While Outlook 2003 has not yet been approved for Enterprise use by the CIO Advisory Council, there is a way to modify the registry of Outlook 2002 to enable this feature. *Please note that Microsoft XP service pack 1 needs to be installed before this feature is available.*

1. Make a backup of your registry.
2. Open the registry editor and locate the following key:
   HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail
3. Click EDIT, NEW, & DWORD VALUE
4. With the new DWord value selected, type ReadAsPlain.
5. Double-click the new value to open it. In the Value Data box, type 1 and then click OK.
6. Click OK and then quit registry editor.

For more information, check out this Microsoft article.

Spam Facts . . .

— The Washington Post claims that 40 percent of all email is Spam.
— Unsolicited email earned the name "spam" because it resembled a Monty Python skit where a chorus of Vikings drowned out other sounds by singing "spam, spam, spam."
— The first spam email may have been sent in 1978 by a Digital Equipment Corporation salesperson to announce a product presentation. Source: The New York Times, February 9, 2003.

McAfee Licensing FAQs

In June 2003, GOT announced a new software licensing agreement with McAfee (Network Associates, Inc.). The agreement has been expanded to include quasi-state government entities (local agencies) and also includes negotiated pricing for McAfee's Active Virus Defense Suite, as well as enhanced technical support. The new agreement is structured differently than the last contract—in the past, agencies went through GOT to purchase McAfee software licenses; now agencies must deal directly with McAfee to acquire the software.

GOT has received many questions regarding the new agreement and has compiled this Frequently Asked Questions (FAQs) document for your convenience:

Q1. Whom do I contact to acquire McAfee Anti-virus Software?
A1. Most agencies have a designated McAfee Agreement contact (see table below). You may want to check with the contact to see if the software has already been acquired through them. Also, another information source is McAfee's regional representative for Kentucky, Brian P. Murawski, who can be contacted via telephone at (972) 987-2183.

Agency	Contact	Agency	Contact
Arts & Humanities	John Detwiler	Local Government	Travis Stewart
Families & Children	Andy Kirby	Natural Resources	Sandi Partin
Finance	Daniel Arnold	Personnel	Connie Gregory
General Government	Omar Marshall	Public Protection	Brian Raley
GOT	Paul Sommerfield/ Shawn Thomas	Revenue	David Carter
Health Services	Adriel Harrod	Tourism	Pamela Powers
Justice	Jerry Wright/Kent Kilgore	Transportation	Bret Blair
Labor	Jeff Maggard	Workforce Development	Tami Dennis
LRC	David Coles		

Q2. I work for the Department of Education, does this agreement apply to my agency?
A2. No. Both the KY Department of Education and the KY Community & Technical College System (KCTCS) have separate agreements with McAfee. Check with your agency CIO or IT contact for more information. All other state and local agencies are eligible to participate in this agreement.

Q3. Can I also install McAfee on my PC at home?
A3. Unless an agency has purchased the Consumer Home Use Option available for an additional fee ($2.40/user), licenses are not valid for home use. GOT has purchased the Consumer Home Use Option for its employees and strongly recommends it for agencies that have staff that access the Commonwealth's networks from home. since the Commonwealth's Enterprise Anti-Virus Policy CIO-073 mandates that home computers connecting to the KIH must be protected by anti-virus software.

Q4. I'm not familiar with McAfee anti-virus products, can I purchase another anti-virus software instead?
A4. No. The McAfee suite of anti-virus products is the enterprise standard for virus protection (Category 5530). No other software is approved for use by state agencies.

Q5. I'm a network administrator and have questions about installing the McAfee software, whom should I contact?
A5. A two year technical support feature is included with the McAfee license. Contact your agency's McAfee contact for McAfee's technical support telephone number or you can access McAfee's online Knowledge Center. There is also information in the Anti-Virus Policy that may be of assistance.

Did you know . . . According to the network protection firm, Internet Security Systems (ISS), the number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. Hackers have lots of opportunities to gain access to systems, especially since 606 software vulnerabilities were made public in the first three months of 2003, with 752 new threats (worms, viruses, Trojans, etc.) identified.

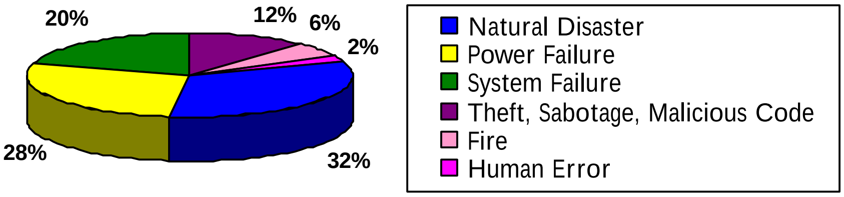
Disaster Recovery 101

Disaster recovery, *business continuity*, *business resumption* . . . these are terms we are all hearing a lot more of since the September 11 tragedies. The Governor's Office for Technology has been dealing with disaster recovery for many years, dating back to the inception of the Commonwealth's first computer behemoth, the IBM mainframe.

Many may be familiar with these terms but may not understand the importance of disaster recovery and the extent of planning necessary to ensure critical information systems are restored after a disastrous event. This article will attempt to answer some of the many questions readers may have regarding disaster recovery and what they can do to prepare and protect their IT systems from a possible disaster.

What is disaster recovery?
Disaster recovery has to do with how an organization prepares to deal with a potential disaster. A disaster recovery plan or DRP (aka Business Continuity Plan—BCP) is the planning document that outlines procedures necessary to lessen the affects of a disaster and to maintain or quickly resume critical systems. The main purpose of the DRP is to provide an effective plan to minimize downtime of critical systems in the event of a major disruption.

What can be considered a disaster?
What constitutes a disaster is usually outlined in an organization's DRP, however, a disaster is typically characterized as any natural or man-made event that creates the inability to provide critical business functions for a predetermined period of time. The major causes of disasters are depicted in the pie chart below:



Isn't the DRP process just a waste of time . . . planning for a disaster that may never happen?
The September 11 tragedies, as well as recent natural disasters, have shown us that we can not be too prepared. It is extremely crucial that an organization have a plan in place that has been thoroughly tested in order for critical business systems to be restored in an acceptable time frame after a disaster. Having an up-to-date, tested plan in place can make the difference in ensuring that vital service delivery to Kentucky citizens is preserved and protected.

Kentucky state government provides many critical services to the people of the Commonwealth. Whether these services deal with providing financial and medical assistance to needy dependent children or issuing food stamps to a hungry family, it is the responsibility of Kentucky state agencies to ensure that a disaster recovery plan is in place for the information systems that support these services. Every Agency should evaluate and categorize their systems to identify those that are critical to operations, and ensure that a disaster recovery plan is developed that will afford timely recovery in the event of a disaster.

In the next issue . . .
Steps for creating and implementing a DRP — who, what, & how.

Did you know . . . According to research conducted by Coopers & Lybrand, of companies that will experience a disaster and do not have a disaster recovery plan in place:
— 40% will face outright collapse.
— 40% will fail within 18 months.
— 12% will fail within 5 years.
— Only 8% will survive the long term.

Cyber Bytes

Vendor Pressure Sidelines Corporate Cyber Security Bill

Federal legislation that would have required businesses to conduct independent security audits and detail the results in their annual reports was tabled recently. The Corporate Information Security Accountability Act of 2003 was tabled by U.S. representatives under pressure by industry groups representing large hardware and software vendors. The vendors are worried that corporate budgets will shift toward consulting and audits and not security products.

— Condensed from an article by Dan Verton in ComputerWorld.

Microsoft's Most Wanted

Microsoft has donated $5 million to a reward fund to nab malicious code writers. According to a Microsoft legal representative, the reward fund isn't a substitute for improving the security of its Windows software, which remains the company's top security priority. The reward program was spawned in recognition that the company needs "to move on multiple fronts" to address the problem.

— Condensed from an article by Patrick Thibodeau & Jaikumar Vijayan in ComputerWorld.

Experts Question Windows Patch Policy

Microsoft recently implemented a new patch policy that has the company sending out monthly alerts designed to ease the burden on network administrators struggling with the frequency of the updates. Microsoft has many critics on its new patch policy. For more information, read the article on ZDNet by Patrick Gray.

Viruses from Outer Space?

While most of us are worrying about malicious code designed by some 16 year-old hacker, a physicist at the Fermi National Accelerator Laboratory in Batavia, Illinois, is concerned about viruses from outer space. Richard Carrigan, Jr. believes those involved in Search for Extraterrestrial Intelligence (SETI) should think about screening SETI signals for malicious code from outer space. For more information check out this article by Leonard David on MSNBC.com

Did you know . . . According to a survey conducted by the Computer Security Institute (CSI), 71 percent of companies responding reported unauthorized access by staff within the company showing that not all intruders originate from the outside.

Microsoft Updates

Microsoft has released the following security updates this month for its operating systems and other software products. GOT recommends that agencies devise procedures to ensure the timely installation of hardware and software patches/updates, as well as the update of virus definition files. A comprehensive list of hardware and software security vulnerabilities can be found on the GOT Security Alert webpage.

Microsoft Security Bulletin MS03-048

Cumulative Security Update for Internet Explorer (824145)

This is a cumulative update that includes the functionality of all the previously-released updates for Internet Explorer 5.01, Internet Explorer 5.5, and Internet Explorer 6.0.

Microsoft Security Bulletin MS03-050

Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run (831527)

A security vulnerability exists in Microsoft Word & Excel that could allow malicious code execution.

Microsoft Security Bulletin MS03-051

Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution (813360)

This bulletin addresses two new security vulnerabilities in Microsoft FrontPage Server Extensions, the most serious of which could enable an attacker to run arbitrary code on a user's system.

Using Windows and Office Update

Microsoft has two websites that help you keep your computer up-to-date on the latest security patches, fixes, and hardware drivers: windowsupdate.microsoft.com and office.microsoft.com/officeupdate, Depending upon the version of Windows you have, you can also access the Windows Update feature from within Windows by clicking on the START button and selecting Windows Update or from within Internet Explorer by selecting TOOLS / WINDOWS UPDATE.

To install the updates, follow this simple process:
1. When you enter the Windows or Office Update site, click on SCAN/CHECK FOR UPDATES.
2. As you browse through the available updates in each category, click ADD to select the update of your choice and add it to the collection of updates you want to install. You can also read a full description of each item by clicking the *Read More* link.
3. When you have selected all the updates you want, click REVIEW AND INSTALL UPDATES, and then click INSTALL NOW.

As always, users should consult their network administrator before applying any updates to their computer.

McAfee Updates

In order to guarantee maximum protection from malicious code, it is extremely important that McAfee virus protection software have the latest virus definition file (DAT) and scan engine installed. The latest DAT can always be found at the GOT Anti-Virus Information webpage. Check with your Agency McAfee contact (see page 4 of this newsletter for a contact list) to be sure you have the most updated anti-virus software and scan engine.

KENTUCKY GOVERNOR'S OFFICE FOR TECHNOLOGY

Division of Security Services
101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502-564-7680
Email: GOTSecurityServices
@ky.gov

We're on the Web!
ky.gov/got/security/

GOT's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security and information systems professionals with timely information on cyber vulnerabilities, information security trends, virus information, and security policies and practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of the GOT Security Policies and Procedures Manual (SPPM), GOT's disaster recovery/ business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, and Unix Solaris & AIX systems. DSS also provides mainframe RACF, computer forensics, and password auditing services to state agencies upon request. If you would like to learn more about the services that DSS provides, visit our web page.

For more information on IT Security, check out the following websites!

www.searchsecurity.com—SearchSecurity provides an aggregation of the best information security content found on the Internet, as well as cutting-edge original featured columns and a highly targeted search engine.

www.fedcirc.gov—Federal Computer Incident Response Center is a central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense (DOD), Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

www.infosecnews.com—InfoSec News is a news service backed by SC Magazine - the largest circulation information security magazine. It is read in more than 50 countries around the world and is published in three separate editions in North America, Europe and the Asia Pacific region. The news service gathers information globally through a network of correspondents and over 200 news services. Key links associated with the news direct you to further sources of information relevant to the news item being reported.

www.incidents.org—Incidents.org is a virtual organization of advanced intrusion detection analyst experts and forensic incident handlers from across the globe. The organization's mission is to provide real time driven security intelligence and support to both organizations and individuals.